The attack graph with bout 20,000 vertices may be generated in less than seven minutes. The result also shows that the methods scale well in the size of attack graphs. The right-hand side shows the running time of each analysis in the size of the attack graph. The result shows that all the analyses require less than a second, which clearly meets the requirement of an interactive analysis. The analyses all scale well with the size of the attack graph. This proves our conjecture that the optimization techniques in databases such as indexing can transparently help to keep analyses efficient. A closer look at the result reveals that the increase in running time is mainly caused by larger results. This may also explain the fact that the incremental update analysis scales differently from the other two (the effect of disabled initial conditions does not change much when the size of the attack graph increases).

[**0090**] FIG. **9** is a block diagram of an aspect of an embodiment of the present invention and FIG. **10** is a flow diagram of an aspect of an embodiment of the present invention. This illustrated system **900** for analyzing attack graphs may use functional modules that may be implemented in software, hardware, or a combination thereof. The hardware can include microprocessors that execute programs stored in memory, discrete logic or programmable logic devices (PLS) such as field programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), application-specific integrated circuits (ASIC), or the like. Some programmable devices may be programmed using software hardware description languages (HDL). The software may include programming languages, application programs, or the like. Each of these options may use configuration data. The modules may reside on one or more tangible computer readable mediums containing a set of computer readable instructions that are executable by one or more processors. Computer readable mediums include RAM, floppy disks, optical disks (such as CD's, DVD's, or HD-DVD's), hard disks, flash drives, or the like.

[**0091**] The modules may include a network configuration information input module **912**, a domain knowledge input module **922**, a network configuration information storage module **914**, a domain knowledge storage module **924**, and a result generation module **940**.

[**0092**] The network configuration information input module **912** is preferably configured to input network configuration information **910** that describes the configuration of a network at **1010**. The network may be any interconnected group or system including a computer network, an electrical network, a telecommunications network, a road network, or the like. Computer networks generally include interconnected computers, hosts, servers, routers, cables and the like. The network information describes elements of the networks and how they connect to each other.

[**0093**] At least part of the network configuration information **910** may describe at least part of the physical structure of the network. The network configuration information **910** may include at least one of the following: host information; host configuration information; application information; network service information; or operating system information; or a combination of the above. In general terms, a host is a computer at a specific location on a computer network. Examples of host configuration information include descriptions and configurations of computer related hardware for host machines within a computer network. Application information may include information about applications such as Microsoft Office applications or Oracle that run on the network. Generally network services are installed on one or more servers to provide shared resources to client computers. They may include administrative functions, security function. Common network services include: authentication servers, directory services. Dynamic Host Configuration Protocol (DHCP), DNS, e-mail, printing, Network file system, and the like. Operating system information preferably includes information about operating systems running in the networks. An operating system (OS) is a set of computer programs that manage the hardware and software resources of a computer. An operating system processes raw system and user input and responds by allocating and managing tasks and internal system resources as a service to users and programs of the system. At the foundation of all system software, an operating system performs basic tasks such as controlling and allocating memory, prioritizing system requests, controlling input and output devices, facilitating networking and managing file systems. Examples of operating systems include: Windows XP and Unix.

[**0094**] The domain knowledge input module **922** is preferably configured to input domain knowledge **920** for the network at **1020**. Domain knowledge **920** may include knowledge about various exploits in the network. An exploit is an action that an attacker can take to advance a goal. An exploit includes but is not limited to: software, chunks of data, or sequences of commands that take advantage of a bug, glitches or vulnerabilities. The exploits are usually intended to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack.

[**0095**] The network configuration information storage module **914** is preferably configured to store network configuration information **910** in at least one network database table **916** at **1030**. Similarly, the domain knowledge storage module **924** is preferably configured to store the domain knowledge **920** in at least one exploit database table **9261040**.

[**0096**] The result generation module **940** is preferably configured to generate a result **950** using the network database table **916** and exploit database table **926** at **1050**. The result **950** may be generated in many ways. For example the network database table **916** and exploit database table **926** could be used to generate another table that describes a complete attack graph. An attack graph is a graph that shows attack paths. An attack path may include a chain of exploits where each exploit lays the groundwork for subsequent exploits.

[**0097**] A result **950** may be generated in response to a query to a database management system **930** that has access to the network database table **916** and exploit database table **926**. A database is a collection of records or data that is stored in a format such as a computer readable table so that a program can consult it to answer queries. The records retrieved in answer to queries may become information that can be used to make decisions. The computer program used to manage and query a database is known as a database management system (DBMS). A database management sys-